

SECTION 2: INFORMATION TECHNOLOGY STANDARDS

2.1 GENERAL

2.1.1	Background	2.1-1
2.1.2	Scope	2.1-1
2.1.3	DoD Technical Architecture Framework for Information Management	2.1-1
2.1.3.1	TAFIM DoD Technical Reference Model	2.1-1
2.1.3.2	Emerging “Integrated” DoD Technical Reference Model	2.1-3
2.1.4	Mandates	2.1-5
2.1.4.1	Year 2000 (Y2K) Compliance	2.1-5
2.1.4.2	Defense Information Infrastructure Common Operating Environment (DII COE)	2.1-5
2.1.5	Organization of Section 2	2.1-6

2.1.1 Background

Section 2 of the JTA is essentially a technical refreshment of Version 1.0 of the JTA. This section is intended as the basis from which to develop the main body of the JTA (i.e., the JTA core). As the JTA evolves, the structure of this section will also evolve to be more reflective of the goal of the JTA structure.

2.1.2 Scope

This section of the JTA establishes the minimum set of rules governing information technology within DoD systems. The scope includes standards for information processing, information transfer, the structure of information and data, human-computer interface standards for information entry and display, and information security standards. Information technology includes any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

2.1.3 DoD Technical Architecture Framework for Information Management

The Technical Architecture Framework for Information Management (TAFIM) version 3.0 is a set of eight volumes consisting of very specific guidance on building and maintaining DoD systems architectures. It describes the process for defining a technical architecture. Volume 2, the Technical Reference Model, as described below and referenced as the TAFIM DoD TRM, is the basis for the structure and standards selected for Section 2 of the JTA.

For applicable systems, the specific guidance in the JTA replaces the general standards guidance in the TAFIM 3.0, Volume 7: Adopted Information Technology Standards (AITS).

2.1.3.1 TAFIM DoD Technical Reference Model

The TAFIM DoD TRM (DoD TRM) and the core set of standards mandated in the JTA define the target technical environment for the acquisition, development, and support of DoD information technology. The purpose of the DoD TRM is to provide a common conceptual framework, and define a common vocabulary so that the diverse components within the DoD can better coordinate acquisition, development, and support of DoD information technology. Interoperability is dependent on the establishment of a common set of services and interfaces that system developers can use to resolve technical architectures and related issues. The DoD TRM structure is intended to reflect the separation of data from applications, and applications from the computing platform – a key principle in achieving open systems. The model is to be used as a guideline for system planning, interoperability, and selecting appropriate standards. The DoD TRM is intended to ensure the use of consistent definitions between the services, domains, interfaces and other

elements needed to define architectural and design components. The model identifies service areas (i.e., sets of capabilities grouped by functions) and their interfaces. The model's separation of the application platform from the application and external environment supports the development of open systems. Portability (i.e., open systems) enables utilization of open standards whereby a conforming application can be used on different and independent platforms.

The model is partitioned into the following: Application Software Entity that includes both mission area and support applications; Application Platform Entity that contains the system support services and operating system services; External Environment; and a number of interfaces. The interfaces provide support for a wide range of applications and configurations, and consist of the following: Application Program Interfaces (APIs), and External Environment Interfaces (EEIs).

The following JTA core services are contained within the DoD TRM's application platform entity:

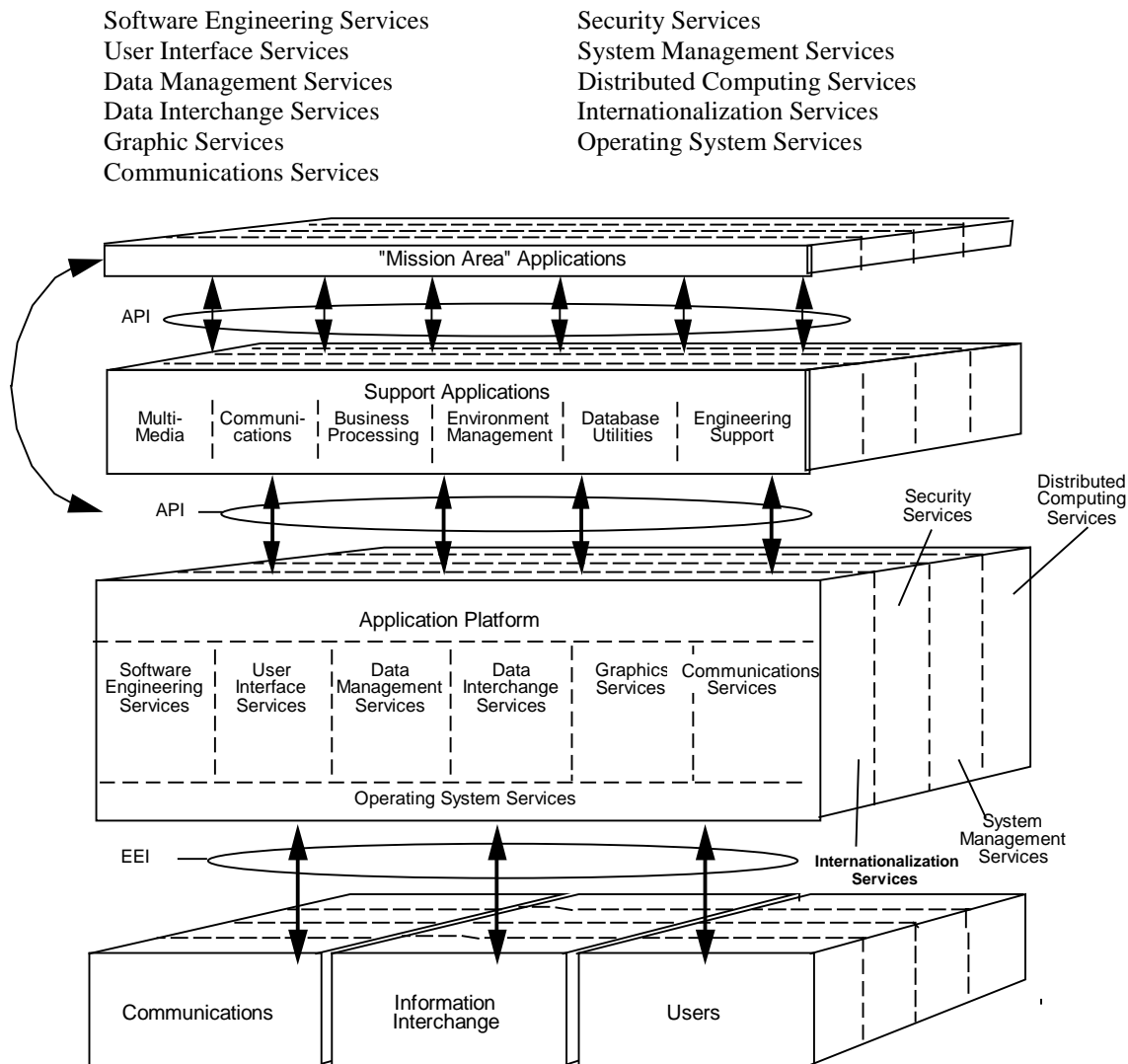


Figure 2.1-1 TAFIM DoD Technical Reference Model

The relationship between the sections in the JTA and the DoD TRM service areas are as follows:

Section 2.2, Information Processing Standards, specifies standards for the User Interface (2.2.2.2.1.2), Data Management (2.2.2.2.1.3), Data Interchange (2.2.2.2.1.4), Graphics (2.2.2.2.1.5), Operating System (2.2.2.2.1.7), Internationalization (2.2.2.2.2.1), and Distributed

Computing (2.2.2.2.4) service areas, and the latter's two subordinate paragraphs become 2.2.2.2.4.1 and 2.2.2.2.4.2 respectively. This section also references, but does not specify any standards for the Software Engineering (2.2.2.2.1.1), Communications (2.2.2.2.1.6), Security (2.2.2.2.2.2), and System Management (2.2.2.2.3) service areas.

Section 2.3, Information Transfer Standards, specifies standards for the Communications (2.3.2.1 through 2.3.2.3) and System Management (2.3.2.4) service areas applicable to both system and network management.

Section 2.4, Information Modeling, Metadata, and Information Exchange Standards, addresses standards for an area that is not currently elaborated, but is supported by engineering support, data management, and software engineering services in the DoD TRM.

Section 2.5, Human-Computer Interface Standards, addresses standards for what is often referred to as TAFIM Volume 8, Version 3.0. The standards specified in Section 2.5 complement those cited for User Interface Services in Section 2.2.2.2.1.2.

Section 2.6, Information Systems Security Standards, specifies security standards that are relevant to the service areas discussed in Sections 2.2, 2.3, and 2.5.

In this version of the JTA, the DoD TRM does not embrace all service areas within the weapon systems domain, and is applicable to the JTA core as described above. In cases where new services are identified, they should be presented to the Technical reference Model Working Group (TRMWG) for adjudication and potential inclusion into the TRM.

2.1.3.2 Emerging “Integrated” DoD Technical Reference Model

To support a more extensive, dynamic and complete set of JTA services, interfaces and platform configurations, an “integrated” DoD TRM (I-DoD TRM) has been developed (Figure 2.1-2). This TRM represents an enhancement to, and uses as a foundation, the TAFIM DoD TRM structure, service features and definitions (as defined in TAFIM Version 3.0, Volume 2, DoD Technical Reference Model). The model also derives interface features that have been identified as essential from the Society of Automotive Engineers (SAE) Generic Open Architecture (GOA) model and other derived models used by certain segments of the Weapons community to support their real-time needs. Thus, the enhanced “integrated” model combines the best of service/interface capabilities and definitions from several existing models. It has the added advantage of providing greater detail in the Application Software and External Environment Entity levels, and is tailorable to accommodate different DoD users and performance needs, both hardware and real-time. Interfaces are defined in Table 2.1-1. The “integrated” model is defined in its entirety in the emerging document, DoD Technical Reference Model, Version 1.0 Draft, dated April 1998.

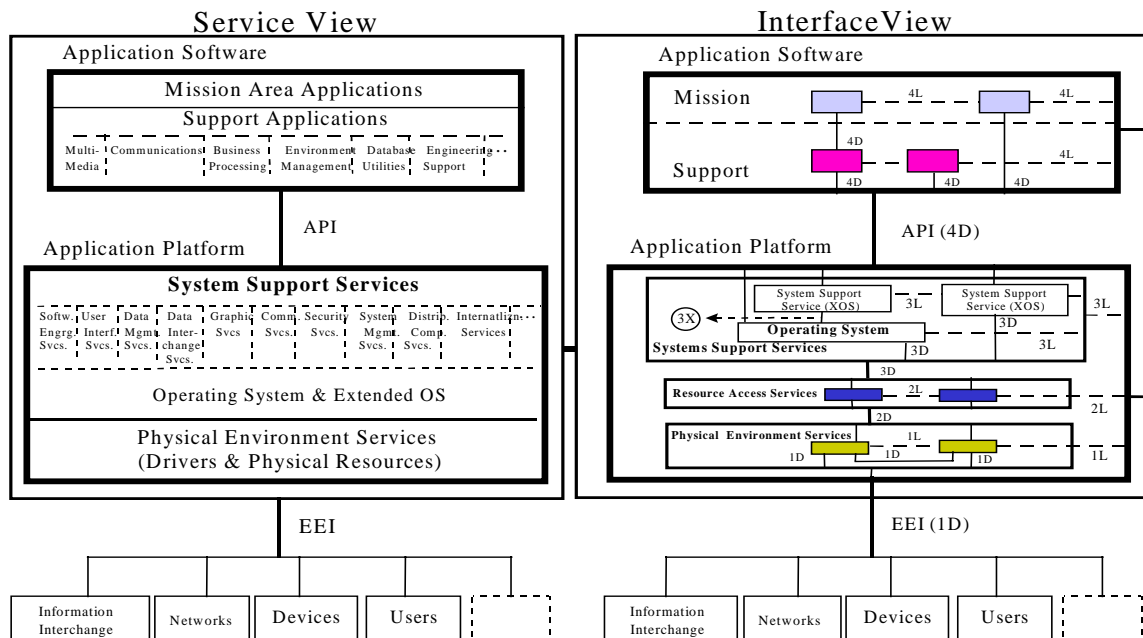


Figure 2.1-2 Integrated DoD Technical Reference Model

Table 2.1-1 Interface Translation Table

Interface Type	Definition
1D	Physical Resources Direct
1L	Physical Resource Logical
2D	Resources-Physical Direct
2L	Resource Access Logical
3D	System Service-Resource Access Direct
3L	System Service Logical
3X	Operating System-Extended OS Direct
4D	Applications-System Services Direct
4L	Applications-Peer Logical

The I-DoD TRM is directly mappable to both the TAFIM DoD TRM services and the interface categories of the GOA model. Transition to and usage of the I-DoD TRM should present no barriers to any current user of existing DoD models (e.g., TAFIM or GOA). DoD ownership of the model, together with its flexibility, will enable it to keep pace with newly emerging service and interface needs ongoing within DoD.

The “integrated” model is currently overseen by the DoD Technical Reference Model Working Group (TRMWG). The TRMWG is a JTA chartered support group assigned to the DISA Center for Standards. The TRMWG’s membership is diverse and composed of the various DoD communities (C4ISR, Weapon Systems, Services, Agencies, and Defense Contractors) requiring a model to support and adjudicate their interoperability and open system needs. The resulting model is consensus driven and viewed as evolutionary to enable it to remain current with emerging DoD needs. The model is consistent with and will continue to support other programs (e.g., the DII COE - see section 2.1.4.2) in addition to the JTA. Upon formal release, the enhanced TRM document together with the JTA is to be used for defining the target

technical environment for DoD information technology needs. The I-DoD TRM document, when approved, will supersede the existing TAFIM Version 3.0, Volume 2, DoD TRM.

2.1.4 Mandates

2.1.4.1 Year 2000 (Y2K) Compliance

To ensure proper data interchange beyond the year 2000, it is DoD policy that all new software and data acquired by the DoD shall be Year 2000 (Y2K) compliant. "Year 2000 compliant" means information technology that accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations. Furthermore, Year 2000 compliant information technology, when used in combination with other information technology, shall accurately process date/time data if the other information technology properly exchanges date/time data with it.¹ Refer to JTA Section 2.4 for guidance on specific date data formats to be used.

DoD policy guidance on this matter can be found in the "DoD Year 2000 Management Plan." The plan is available on the World Wide Web at:

<http://www.dtic.mil/c3i/>

For procurement and acquisition purposes, the General Services Administration (GSA) has made available the following documents:

1. "Recommended Year 2000 Contract Language (1996-09-11)"
2. "Federal Acquisition Regulation Interim Rule on the Year 2000 (1997-01-02)"

These documents can be used by contracting officers to help ensure that acquired products and services are Y2K compliant. They are available on the GSA World Wide Web site at:

<http://www.itpolicy.gsa.gov/>

2.1.4.2 Defense Information Infrastructure Common Operating Environment (DII COE)

The Common Operating Environment (COE) concept is described in the Integration and Runtime Specification (I&RTS), Version 3.0, 1 July 1997. The Defense Information Infrastructure COE (DII COE) is implemented with a set of modular software that provides generic functions or services, such as operating system services. These services or functions are accessed by other software through standard APIs. The DII COE may be adapted and tailored to meet the specific requirements of a domain. COE Implementations provide standard, modular software services that are consistent with the service areas identified in the DoD Technical Reference Model. Application programmers then have access to these software services through standardized APIs.

The DII COE, as defined in the DII COE I&RTS Version 3.0, is fundamental to a Joint System Architecture (JSA). In the absence of a JSA, the JTA mandates that all Command, Control, Communications, Computers, and Intelligence (C4I) systems shall use the DII COE. The strict definition of C4I, as given in JTA 1.0, is expanding to cover information technology areas that cut across JTA Version 2.0 domain boundaries. The DII COE mandate is therefore intended for all applicable systems. All applications of a system which must be integrated into the DII shall be at least DII COE I&RTS level 5 compliant (software is segmented, uses DII COE Kernel, and is installed via COE tools) with a goal of achieving level 8.

¹ August 1, 1997 Interim FAR Rule on Year 2000 Compliance

The DII COE implements the appropriate JTA standards applicable to the COE functionality. The DII COE implementation will continue to evolve in compliance with all applicable JTA specifications, standards, and source references. Additional functionality not contained in the DII COE is subject to the JTA mandate.

2.1.5 Organization of Section 2

The Information Technology section of the JTA consists of six sections. The first section is the overview. The next sections are: (2.2) Information Processing Standards; (2.3) Information Transfer Standards; (2.4) Information Modeling, Metadata, and Information Exchange Standards; (2.5) Human-Computer Interface Standards; and (2.6) Information Systems Security Standards.

Information Processing Standards - Section 2.2 describes government and commercial information processing standards the DoD shall use to develop integrated, interoperable systems that meet the Warfighters' information processing requirements.

Information Transfer Standards - Section 2.3 describes the information transfer standards and profiles that are essential for information transfer interoperability and seamless communications. This section mandates the use of the open-systems standards used for the Internet and the Defense Information System Network (DISN).

Information Modeling, Metadata, and Information Exchange Standards - Section 2.4 describes the use of integrated information modeling and mandates applicable standards. Information modeling consists of Activity and Data Modeling. This section explains the use of the DoD Command and Control (C2) Core Data Model (C2CDM) and the Defense Data Dictionary System (DDDS), formerly the Defense Data Repository System (DDRS). This section also mandates information standards including message formats.

Human-Computer Interface Standards - Section 2.5 provides a common framework for Human-Computer Interface (HCI) design and implementation in DoD systems. The objective is the standardization of user interface implementation options, enabling DoD applications to appear and behave in a reasonably consistent manner. The section specifies HCI design guidance, mandates, and standards.

Information Systems Security Standards - Section 2.6 prescribes the standards and protocols to be used to satisfy security requirements. This section provides the mandated and emerging security standards that apply to JTA Sections 2.2 through 2.5. Section 2.6 is structured to mirror the overall organization of the JTA so that readers can easily link security topics with the related JTA subject areas.